Description

Drive apparatus for safety-critical components, and a corresponding method

The present invention relates to a drive apparatus for open-loop or closed-loop control of a safety-critical component having a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, a first control device for reception of an input signal and emission of a first drive signal, and a second control device for reception of the input signal and for emission of a second drive signal. The present invention also relates to a corresponding method for open-loop or closed-loop control of a safety-critical component.

Many safety applications require a very short reaction time for processing of an EMERGENCY-OFF demand. Although present-day modern safety appliances generally use microcontrollers and internal functions can therefore be processed very quickly, filter algorithms have to be used, because of burst and RF interference, in order to achieve the maximum availability. Further boundary effects such as compensation for the cable capacity and dynamic input testing in the end lead to relatively long evaluation times.

A drive apparatus which has two series-connected switches in order to satisfy the hardware redundancy requirement, with the switches each being electrically connected to their own microcontroller via a relay drive, is known from the report "Not-Aus-Schaltgeräte, Schutztürwächter [Emergency-off switching devices, guard door monitors] Announcement Pilz NSG-D-1-051-07/00, XX, XX, July 2000 (2000-07), pages 1 to 4, XP 000961973" One input of each of the microcontrollers is electrically connected to an emergency-off switch, and they are

formed alongside one another, with equal authority. The switches can each be controlled via the associated microcontroller. The switches are controlled as a function of the need to switch off a safety-critical component.

Furthermore, a safety device in which a sensor apparatus is electrically connected to two evaluation devices is known from German Laid Open Specification DE 44 09 541 A1. One output of each evaluation unit is electrically connected to a switch which is in the form of an auxiliary contactor. A timer is arranged in the signal path between one evaluation unit and one auxiliary contactor, by means of which timer it is possible to switch off a downstream main circuit via the auxiliary contactor, with a delay.

A further problem is represented by the fact that, in safety appliances from Category SIL3 with respect to the European IEC Standard 615 08, two controllers must always be used for hardware redundancy and fault tolerance reasons.

The applicant has solved this problem, in the case of safety appliances, by using two controllers with identical hardware and

The object of the present invention is thus to propose a drive apparatus and a corresponding method for open-loop or closed-loop control of a safety-critical component, whose reaction time is shortened on average.

According to the invention, this object is achieved by a drive apparatus for open-loop or closed-loop control of a safety-critical component having a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, a first control device for reception of an input signal and emission of a first drive signal, and a second control device for reception of the input signal and for emission of a second drive signal, wherein the first switch in the switching device can be driven by the first control device and the second switch in the switching device can be driven by the second control device. The first and the second switch are driven with a time-offset with respect to one another. Furthermore, the first and the second control device operate on the master/slave principle, thus resulting in a defined time offset.

The invention also provides a method for open-loop or closed-loop control of a safety-critical component by provision of a switching device which has a first switch and a second switch, which is connected in series with the first, for switching the safety-critical component, provision of a first control device, which is connected to the switch, and of a second control device which is connected to the second switch, reception of an input signal and emission of a first drive signal from the first control device to the first switch in the switching device on the basis of the input signal, wherein the second control device emits a second drive signal to the second switch in the switching device on the basis of the input signal.

The invention is based on the idea that the output should be switched off irrespective of which of the

switches is turned off first all. Since both controllers or control devices now drive the series circuit comprising the two switches and this results in the outputs of the controllers being AND-linked, the output to the switching device is switched off in all cases with the shorter reaction time of the two controllers.

One positive side-effect of this time-offset switching is that simultaneous welding of the two switches, for example contactors, can be precluded. The EMERGENCY-OFF function is thus still ensured even after welding of one of the contacts of the switches.

The time-offset switching-off of the switches also has the advantage that approximately the same life can be expected of both switches. This is because each switch is switched off with equal frequency, statistically on average, with and without current flowing through it.

The first and the second switch in the switching device are preferably each formed by a relay or a contactor. Alternatively, the first and the second switch may, however, also be in the form of semiconductor switches or may comprise an optocoupler.

The time offset is then, specifically, governed by the time period which the master requires in order to make the slave aware of an event.

An electrical machine with a load circuit is advantageously equipped with the said drive apparatus according to the invention. In this case, the drive apparatus may

Patent Claims

1. A drive apparatus for open-loop or closed-loop control of a safety-critical component having

- a switching device which has a first switch (S1) and a second switch (S2), which is connected in series with the first, for switching the safety-critical component,
- a first control device (C1) for reception of an input signal and emission of a first drive signal, and
- a second control device (C2) for reception of the input signal and for emission of a second drive signal, wherein
- the first switch (S1) in the switching device can be driven by the first control device (C1) and the second switch (S2) in the switching device can be driven by the second control device (C2),

characterized in that

- the first switch (S1) and the second switch (S2) can be driven with a time offset with respect to one another, and the first and the second control device operate on the master/slave principle.

2. The drive apparatus as claimed in claim 1, wherein the first and the second switch are in each case a relay or a contactor.

3. The drive apparatus as claimed in claim 1, wherein the first and the second switch are in each case a semiconductor switch.

4. The drive apparatus as claimed in claim 1, wherein the first and the second switch in each case comprise an optocoupler.

5. An electrical machine having a load circuit and a drive apparatus as claimed in one of the preceding claims.

6. The electrical machine as claimed in claim 5, also having an emergency-off switch (X) for supplying the input signal.

7. A method for open-loop or closed-loop control of a safety-critical component by:

- provision of a switching device which has a first switch (S1) and a second switch (S2), which is connected in series with the first, for switching the safety-critical component,
- provision of a first control device (C1), which is connected to the switch (S1), and of a second control device (C2) which is connected to the second switch (S2),
- reception of an input signal,
- emission of a first drive signal from the first control device (C1) to the first switch (S1) in the switching device on the basis of the input signal, and
- emission of a second drive signal from the second control device (C2) to the second switch (S2) in the switching device on the basis of the input signal,

characterized in that

- the first and the second drive signal are emitted with a time offset with respect to one another, wherein the first and the second drive signal are produced using a master/slave process as a function of the input signal, thus resulting in the defined time offset.

8. The method as claimed in claim 7, wherein the switching device is used to switch a load circuit of an electrical machine.

9. The method as claimed in one of claims 7 or 8, wherein the input signal is produced by an emergency-off switch (X).

Beschreibung

Ansteuervorrichtung für sicherheitskritische Komponenten und entsprechendes Verfahren

Die vorliegende Erfindung betrifft eine Ansteuervorrichtung zum Steuern oder Regeln einer sicherheitskritischen Komponente mit einer Schalteinrichtung, die einen ersten Schalter und einen zweiten, mit dem ersten in Reihe verbundenen Schalter zum Schalten der sicherheitskritischem Komponente aufweist, einer ersten Steuerungseinrichtung zur Aufnahme eines Eingangssignals und Ausgabe eines ersten Ansteuersignals und einer zweiten Steuerungseinrichtung zur Aufnahme des Eingangssignals und Ausgabe eine zweiten Ansteuersignals. Darüber hinaus betrifft die vorliegende Erfindung ein entsprechendes Verfahren zum Steuern oder Regeln einer sicherheitskritischen Komponente.

Bei vielen sicherheitstechnischen Anwendungen wird eine sehr geringe Reaktionszeit zur Verarbeitung einer NOTAUS-Anforderung benötigt. Obwohl die heutigen modernen Sicherheitsgeräte in der Regel Mikrocontroller benutzen und deshalb interne Funktionen sehr schnell abgearbeitet werden können, müssen wegen Burst- und HF-Störungen Filteralgorithmen verwendet werden, um eine maximale Verfügbarkeit zu erzielen. Weitere Randeffekte wie die Kompensation der Kabelkapazität und dynamische Eingangsprüfung führen letztlich zu relativ langen Auswertezyklen.

Aus dem Bericht "Not-Aus-Schaltgeräte, Schutztürwächter; Announcement Pilz NSG-D-1-051-07/00, XX, XX, Juli 2000 (2000-07), Seiten 1 bis 4, XP 000961973" ist eine Ansteuervorrichtung bekannt, welche im Hinblick auf das Hardwareredundanzerfordernis zwei in Reihe geschaltete Schalter aufweist, die jeweils über eine Relaisansteuerung mit einem eigenen µController elektrisch verbunden sind. Die µController sind jeweils mit einem Eingang mit einem Not-Aus-Schalter elekt-

risch gekoppelt und gleichberechtigt nebeneinander ausgebildet. Die Schalter sind jeweils über den zugeordneten µController steuerbar. Abhängig von einem erforderlichen Abschalten einer sicherheitskritischen Komponente werden die Schalter gesteuert.

Des Weiteren ist aus der deutschen Offenlegungsschrift DE 44 09 541 A1 eine sicherheitstechnische Einrichtung bekannt, bei der eine Sensorvorrichtung mit zwei Auswerteeinrichtungen elektrisch verbunden ist. Jede Auswerteeinheit ist mit einem Ausgang mit einem als Hilfsschütz ausgebildeten Schalter elektrisch verbunden. In die Signalstrecke zwischen einer Auswerteeinheit und einem Hilfsschütz ist ein Zeitglied angeordnet, mit dem das verzögerte Abschalten eines nachgeordneten Hauptstromkreises über den Hilfsschütz durchgeführt werden kann.

Ein weiteres Problem stellt die Tatsache dar, dass in Sicherheitsgeräten ab der Kategorie SIL3 bezogen auf die europäische Norm IEC 615 08 immer zwei Controller aus Gründen der Hardwareredundanz und Fehlertoleranz eingesetzt werden müssen.

Seitens des Anmelders wurde dieses Problem dadurch gelöst, dass bei Sicherheitsgeräten zwei von der Hardware identische

Die Aufgabe der vorliegenden Erfindung besteht somit darin, eine Ansteuervorrichtung und ein entsprechendes Verfahren zum Steuern oder Regeln einer sicherheitskritischen Komponente mit durchschnittlich verkürzter Reaktionszeit vorzuschlagen.

Erfindungsgemäß wird diese Aufgabe gelöst durch eine Ansteuervorrichtung zum Steuern oder Regeln einer sicherheitskritischen Komponente mit einer Schalteinrichtung, die einen ersten Schalter und einen zweiten, mit dem ersten in Reihe verbundenen Schalter zum Schalten der sicherheitskritischen Komponente aufweist, einer ersten Steuerungseinrichtung zur Aufnahme eines Eingangssignals und Ausgabe eines ersten Ansteuersignals und einer zweiten Steuerungseinrichtung zur Aufnahme des Eingangssignals und Ausgabe eines zweiten Ansteuersignals, wobei der erste Schalter der Schalteinrichtung von der ersten Steuerungseinrichtung und der zweite Schalter der Schalteinrichtung von der zweiten Steuereinrichtung ansteuerbar sind. Der erste und zweite Schalter werden zeitversetzt zueinander angesteuert. Ferner arbeiten die erste und zweite Steuerungseinrichtung nach dem Master-Slave-Prinzip, wodurch sich ein definierter Zeitversatz ergibt.

Ferner wird erfindungsgemäß bereitgestellt ein Verfahren zum Steuern oder Regeln einer sicherheitskritischen Komponente durch Bereitstellen einer Schalteinrichtung, die einen ersten Schalter und einen zweiten, mit dem ersten in Reihe verbundenen Schalter zum Schalten der sicherheitskritischen Komponente aufweist, Bereitstellen einer ersten Steuerungseinrichtung, die mit dem Schalter verbunden ist, und einer zweiten Steuerungseinrichtung, die mit dem zweiten Schalter verbunden ist, Aufnehmen eines Eingangssignals und Ausgeben eines ersten Ansteuersignals von der ersten Steuerungseinrichtung an den ersten Schalter der Schalteinrichtung auf der Basis des Eingangssignals, wobei auf der Basis des Eingangssignals ein zweites Ansteuersignal von der zweiten Steuerungseinrichtung an den zweiten Schalter der Schalteinrichtung ausgegeben wird.

Der Erfindung liegt der Gedanke zugrunde, dass der Ausgang abgeschaltet werden soll, unabhängig davon, welcher der Schalter zuerst abgesteuert wird. Dadurch, dass nun beide Controller beziehungsweise Steuerungseinrichtungen die Reihenschaltung aus den beiden Schaltern ansteuern und somit eine UND-Verknüpfung der Ausgänge der Controller gegeben ist, wird der Ausgang an der Schalteinrichtung auf alle Fälle mit der geringeren Reaktionszeit der beiden Controller abgeschaltet.

Ein positiver Nebeneffekt dieses zeitversetzten Schaltens ist, dass ein gleichzeitiges Verschweißen der beiden Schalter, z. B. Schütze, ausgeschlossen werden kann. Die NOTAUS-Funktion ist damit auch nach dem Verschweißen eines der Kontakte der Schalter noch gewährleistet.

Das zeitversetzte Abschalten der Schalter hat weiterhin den Vorteil, dass für beide Schalter ungefähr gleiche Lebensdauern zu erwarten sind. Dies liegt daran, dass im statistischen Mittel jeder Schalter ebenso häufig im stromfreien wie im bestromten Zustand abgeschaltet wird.

Vorzugsweise wird der erste und zweite Schalter in der Schalteinrichtung jeweils durch ein Relais oder einen Schütz realisiert. Alternativ kann der erste und zweite Schalter aber auch als Halbleiterschalter ausgelegt sein oder einen Optokoppler umfassen.

Speziell entsteht der Zeitversatz durch die Zeitdauer, die der Master benötigt, um den Slave von einem Ereignis in Kenntnis zu setzen.

Vorteilhafterweise wird eine elektrische Maschine mit einem Lastkreis mit der genannten, erfindungsgemäßen Ansteuervorrichtung ausgestattet. Dabei kann die Ansteuervorrichtung

Patentansprüche

1. Ansteuervorrichtung zum Steuern oder Regeln einer sicherheitskritischen Komponente mit
   - einer Schalteinrichtung, die einen ersten Schalter (S1) und einen zweiten, mit dem ersten in Reihe verbundenen Schalter (S2) zum Schalten der sicherheitskritischen Komponente aufweist,
   - einer ersten Steuerungseinrichtung (C1) zur Aufnahme eines Eingangssignals und Ausgabe eines ersten Ansteuersignals und
   - einer zweiten Steuerungseinrichtung (C2) zur Aufnahme des Eingangssignals und Ausgabe eines zweiten Ansteuersignals, wobei
   - der erste Schalter (S1) der Schalteinrichtung von der ersten Steuerungseinrichtung (C1) und der zweite Schalter (S2) der Schalteinrichtung von der zweiten Steuereinrichtung (C2) ansteuerbar sind,

   d a d u r c h  g e k e n n z e i c h n e t ,  d a s s
   - der erste Schalter (S1) und der zweite Schalter (S2) mit Zeitversatz zueinander ansteuerbar sind und die erste und zweite Steuerungseinrichtung nach dem Master/Slave-Prinzip arbeiten.

2. Ansteuervorrichtung nach Anspruch 1, wobei der erste und zweite Schalter jeweils ein Relais oder ein Schütz ist.

3. Ansteuervorrichtung nach Anspruch 1, wobei der erste und zweite Schalter jeweils ein Halbleiterschalter ist.

4. Ansteuervorrichtung nach Anspruch 1, wobei der erste und zweite Schalter jeweils einen Optokoppler umfasst.

5. Elektrische Maschine mit einem Lastkreis und einer Ansteuervorrichtung nach einem der vorhergehenden Ansprüche.

6. Elektrische Maschine nach Anspruch 5 mit weiterhin einem Not-Aus-Schalter (X) zum Liefern des Eingangssignals.

7. Verfahren zum Steuern oder Regeln einer sicherheitskritischen Komponente durch
   - Bereitstellen einer Schalteinrichtung, die einen ersten Schalter (S1) und einen zweiten, mit dem ersten in Reihe verbundenen Schalter (S2) zum Schalten der sicherheitskritischen Komponente aufweist,
   - Bereitstellen einer ersten Steuerungseinrichtung (C1), die mit dem Schalter (S1) verbunden ist, und einer zweiten Steuerungseinrichtung (C2), die mit dem zweiten Schalter (S2) verbunden ist,
   - Aufnehmen eines Eingangssignals,
   - Ausgeben eines ersten Ansteuersignals von der ersten Steuerungseinrichtung (C1) an den ersten Schalter (S1) der Schalteinrichtung auf der Basis des Eingangssignals und
   - Ausgeben eines zweiten Ansteuersignals von der zweiten Steuerungseinrichtung (C2) an den zweiten Schalter (S2) der Schalteinrichtung auf der Basis des Eingangssignals,

   d a d u r c h g e k e n n z e i c h n e t , d a s s
   - das erste und zweite Ansteuersignal zeitversetzt zueinander ausgegeben werden, wobei das erste und das zweite Ansteuersignal in einem Master/Slave-Prozess in Abhängigkeit von dem Eingangssignal erzeugt werden, wodurch sich der definierte Zeitversatz ergibt.

8. Verfahren nach Anspruch 7, wobei mit der Schalteinrichtung ein Lastkreis einer elektrischen Maschine geschaltet wird.

9. Verfahren nach einem der Ansprüche 7 oder 8, wobei das Eingangssignal von einem Not-Aus-Schalter (X) geliefert wird.

GERMAN TRANSLATION AID

Es bedeutet: (It means:)

X: Druckschriften, die Neuheit oder Erfindungshöhe allein in Frage stellen

(Publications, which question novelty or just obviousness)

Y: Druckschriften, die die Erfindungshöhe züsammen mit anderen Druckschriften in Frage stellen

(Publications which, together with other publications, question obviousness)

A: Allgemein zum Stand der Technik, technologischer Hintergrund

(General state of the art, technological background)

O: Nicht-schriftliche Offenbarung, z. B. ein in einer nachveröffentlichten Druckschrift abgedruckter Vortrag, der vor dem Anmelde- oder Prioritätstag öffentilich gehalten wurde

(Non-written disclosure, for example, a printed post publication of a lecture which was publicly made before the filing date or priority date)

P: Im Prioritätsintervall veröffentichte Druckschriften

(Publications publicized in a priority interval)

T: Nachveröffentlichte, nicht kollidierende Druckschriften , die die Theorie der angemeldeten Erfindung betreffen und für ein besseres Verständnis der angemeldeten Erfindung nützlich sein können bzw. zeigen daß der angemeldeten Erfindung zugrunde liegende Gedankengänge oder Sachverhalte falsch sein könnten

(Post publications, not anticipating publications, which refer to the theory of the filed invention and which refer could be useful for a better understanding or, as the case may be, which could show that reasoning or facts of the filed invention are incorrect)

E: Ältere Anmeldungen gemäß §3 Abs.2 PatG (bei Recherchen nach § 43 PatG); ältere Patentanmeldungen oder ältere Gebrauchsmuster gemäß § 15 GbmG (bei Recherchen nach § 7 GbmG)

(Older applications under § 3 section 2 PatG (inquiries under § 43 PatG); older patent applications ir patents under § 15 GbmG (inquiries under § 7 GmbG))

D: Druckschriften, die bereits in der Patentmeldung genannt sind

(Publications, which are cited in the patent application)

L: Aus besonderen Gründen genannte Druckschriften, z. B. zum Veröffentlichungstag einer Entgegenhaltung oder bei Zweifeln an der Priorität.

(Publications which are cited for a particular reason, for example, relative to the publication date of a reference or cast doubt on the priority)

Veröff: Veröffentlichungstag einer Druckschrift im Prioritätsintervall

(Publication date of a publication in a priority interval)

nr: Nicht recherchiert, da allgemein bekannter Stand der Technik, oder nicht recherchierbar

(Not searched, because it is known state of the art, or cannot be searched)

=: Druckschriften, die auf dieselbe Ursprungsanmeldung zuzrückgehen ("Patentfamilien"), oder auf die sich Referate oder Abstracts beziehen.

(Publications, which refer to the same original application ("patent family"), or which are referred to in reviews or abstracts.)

"-": Nichts ermittelt

(Nothing discovered)

Hier sind die Ansprüche unter Zuordnung zu den in Spalte 2 genannten relevanten Stellen angegeben.

(The claims are stated herein which refer to the relevant positions recited in column 2.)

| | |
|---|---|
| Seite | (page) |
| Zeile | (line) |
| Abbildungen | (Drawings) |
| Spalte | (Column) |
| Absatz | (Paragraph) |
| Zumsammenfassung | (Abstract of Disclosure) |